IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Andrew G. Tucker et al.

Application No.: 10/769,415 Confirmation No.: 8014

Filed: January 30, 2004 Art Unit: 2431

For: FINE-GRAINED PRIVILEGES IN OPERATING SYSTEM PARTITIONS Examiner: M. R. Vaughan

APPEAL BRIEF

MS Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Pursuant to 37 CFR § 41.37, please consider the following Appellant's Brief in the referenced application currently before the Board of Patent Appeals and Interferences.

TABLE OF CONTENTS

This brief contains items under the following headings as required by 37 C.F.R. § 41.37 and M.P.E.P. § 1205.2:

I. REAL PARTY OF INTEREST 4
II. RELATED APPEALS AND INTERFERENCES 4
III. STATUS OF CLAIMS 4
IV. STATUS OF AMENDMENTS 5
V. SUMMARY OF CLAIMED SUBJECT MATTER 5
VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL 7
VII. ARGUMENT 7
VIII. CONCLUSION 12
CLAIMS APPENDIX 13
EVIDENCE APPENDIX 17
RELATED PROCEEDINGS APPENDIX 18

TABLE OF AUTHORITIES

Cases

Elekta Instruments, S.A. v. O.U.R. Sci. Int'l, Inc., 214 F.3d 1302 (Fed. Cir. 2002) 8
In re *American Academy of Science Tech. Center*, 367 F.3d 1359, 1363 (Fed. Cir. 2004) 9
In re Bond, 910 F.2d 831, 833 (Fed. Cir. 1990) 9
Innova/Pure Water, Inc. v. Safari Water Filtration Systems, Inc., 381 F.3d 1111 (Fed. Cir. 2004) 8
Markman v. Westview Instruments, 52 F.3d 967 (Fed. Cir. 1995) 10
Merk & Co., Inc. v. Teva Pharmaceuticals USA, Inc., 395 F.3d 1364, 1372 (Fed. Cir. 2005) 8
Net MoneyIN v. Verisign, 545 F.3d 1359, 1371 (Fed. Cir. 2008) 11
Phillips v. AWH Corp., 415 F.3d 1303, 1315 (Fed. Cir. 2005) 10
Richardson v. Suzuki Motor Co., 868 F.2d 1226, 1236 (Fed. Cir. 1989) 8
Verdegaal Bros. v. Union Oil Co. of California, 814 F.2d 628, 631 (Fed. Cir. 1987) 8

Statutes

35 U.S.C. § 102 ..... 7, 11, 12

I. REAL PARTY OF INTEREST

The real party in interest for this appeal is Oracle America, Inc., formerly known as Sun Microsystems, Inc. An Assignment transferring all interest in the referenced application from the inventor to Sun Microsystems, Inc. was filed with the USPTO on December 27, 2005. The Assignment is recorded at Reel 017143, Frame 0410.

II. RELATED APPEALS AND INTERFERENCES

To the best of the knowledge of the Appellants and Appellants' legal representative, there are no other appeals or interferences that will directly affect, be affected by, or have a bearing on the decision of the Board of Patent Appeals and Interferences ("The Board") in this appeal.

III. STATUS OF CLAIMS

U.S. Application Serial No. 10/769,415 ("the '415 Application") was filed on August 19, 2005. As filed, the '415 Application included claims 1-27. In a preliminary amendment filed on February 12, 2007, claims 1-26 were cancelled, and claims 28-53 were added. In a response to election of species requirement filed on March 19, 2009, species IV was selected, which includes claims 34, 35, 40, 47, 48, and 53. Claims 27-29, 37, 41-42, and 50 were found to be generic. In an amendment dated September11, 2009, claims 27-29, 34-35, 37, and 40 were cancelled without prejudice or disclaimer, and claims 54-58 were added. Accordingly, claims 41, 47, 48, 50, and 53-58 are pending in the '415 Application. Claims 41 and 54 are independent. The remaining claims depend, directly or indirectly, from the independent claims.

All the pending claims were rejected in a Final Office Action dated December 8, 2009 ("Final Office Action").

Claims 41, 47, 48, 50, and 53-58 are on appeal.

IV. STATUS OF AMENDMENTS

All of the amendments have been entered and considered by the Examiner. Appellants did not file an Amendment after the Final Rejection. The pending claims of record are present in the Claims Appendix.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The following discussion summarizes the content of the claimed subject matter. The references to the Specification made below should not be construed as the only location in the Specification which support or discuss the respective limitation.

Independent claim 41 discloses a computer readable medium including a set of one or more instructions which, when executed my one or more processors, causes the one or more processors to perform a method. *See, e.g.,* Specification, page 31, lines 16-23; Fig. 4: 400. The method includes, in an operating system environment controlled by a single operating system kernel instance (*see, e.g,* Specification, page 14, lines 20-24; Fig. 1: 15), establishing a global zone. *See, e.g.,* Specification, page 12, lines 16-20; Fig. 1:130. The global zone includes a first non-global zone. *See, e.g.,* Specification, page 12, lines 16-20; Fig. 1:140. The first non-global zone includes a first file system. *See, e.g.,* Specification, page 13, lines 3-7; Fig. 1: 180(a). The global zone includes a second file system. *See, e.g.,* Specification, page 13,lines 3-7; Fig. 1:180(b). The method also includes receiving, from a first process, a first request to perform a first operation. *See, e.g.,* Specification, page 18, lines 13-17; Fig. 3D: 372. The first process is associated with a first set of privileges and is executed by at least one of the one or more

processors. *See, e.g.,* Specification, page 30, lines 2-6; Fig. 3B2:354. The first set of privileges restricts the first process to the first non-global zone. *See, e.g.,* Specification, page 2-6; Fig. 3B2:354. The method also includes, in response to the first request, determining whether performing the first operation is within the first set of privileges. *See, e.g.,* Specification, page 30, lines 5-7; Fig.3B2:354. The method also includes denying the first request if performing the first operation is not within the first set of privileges. *See, e.g.,* Specification, page 30, lines 7-8; Fig. 3B2:360.

Independent claim 54 discloses a system. The system includes at least one processor. *See, e.g.,* Specification, page 33, lines 11-14; Fig. 4:404. The system also includes a computer readable medium including a set of instructions which, when executed by the at least one processor, cause the at least one processor to perform a method. *See, e.g.,* Specification, page 31, lines 16-23; Fig. 4: 400. The method includes, in an operating system environment controlled by a single operating system kernel instance (*see, e.g,* Specification, page 14, lines 20-24; Fig. 1: 15), establishing a global zone. *See, e.g.,* Specification, page 12, lines 16-20; Fig. 1:130. The global zone includes a first non-global zone. *See, e.g.,* Specification, page 12, lines 16-20; Fig. 1:140. The first non-global zone includes a first file system. *See, e.g.,* Specification, page 13, lines 3-7; Fig. 1: 180(a). The global zone includes a second file system. *See, e.g.,* Specification, page 13,lines 3-7; Fig. 1:180(b). The method also includes receiving, from a first process, a first request to perform a first operation. *See, e.g.,* Specification, page 18, lines 13-17; Fig. 3D: 372. The first process is associated with a first set of privileges and is executed by at least one of the one or more processors. *See, e.g.,* Specification, page 30, lines 2-6; Fig. 3B2:354. The first set of privileges restricts the first process to the first non-global zone. *See, e.g.,* Specification, page 2-6; Fig. 3B2:354. The method also includes, in response to the first

request, determining whether performing the first operation is within the first set of privileges. *See, e.g.,* Specification, page 30, lines 5-7; Fig.3B2:354. The method also includes denying the first request if performing the first operation is not within the first set of privileges. *See, e.g.,* Specification, page 30, lines 7-8; Fig. 3B2:360.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The rejection to be reviewed on this appeal is the rejection of claims 41, 47, 48, 50, and 53-58 under 35 U.S.C. § 102 as being anticipated by U.S. Patent Publication No. 2003/0172109 ("Dalton").

VII. ARGUMENT

In this Appeal, Appellant argues that claims 41, 47, 48, 50, and 53-58 are not anticipated over Dalton, whether viewed separately or in combination, for at least the reasons given below. Independent claim 41 is representative of claims 41, 47, 48, 50, and 53-58.

Briefly, independent claim 1 requires, at least in part, *(i)* a global zone including a first file system; and *(ii)* a non-global zone including a second file system. A first request to perform a first operation is received from a first process. The first process is associated with a first set of privileges, which restrict the first process to the non-global zone. A determination is made as to whether performing the first operation is within the first set of privileges. When it is not within the first set of privileges, the request is denied.

Briefly, Dalton discloses an operating system on a host with logically protected computing compartments. *See* Dalton, para. [0022]. The host includes a host file system, and

each computing compartment is provided access to "a restricted subset of the host file system." *See* Dalton, para. [0023].

Turning to the rejection, "[a] claim is anticipated only if *each and every element* as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631 (Fed. Cir. 1987) (emphasis added). Further, "[t]he identical invention must be shown in as complete detail as is contained in the claims." *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236 (Fed. Cir. 1989). Appellants assert that Dalton fails to disclose all the limitations of the pending independent claims.

1. The Examiner has failed to properly consider the terms "first file system" and "second file system"

Applicants respectfully assert that "[a] claim construction that gives meaning to all the terms of the claim is preferred to one that does not do so." *See Merk & Co., Inc. v. Teva Pharmaceuticals USA, Inc.*, 395 F.3d 1364, 1372 (Fed. Cir. 2005) (citing *Elekta Instruments, S.A. v. O.U.R. Sci. Int'l, Inc.*, 214 F.3d 1302 (Fed. Cir. 2002)). In construing the definition of a first and a second file system, the Examiner has erred.

1a. Proper construction of "file system"

"[T]he words of a claim are generally given their ordinary and customary meaning," specifically the ordinary and customary meaning is considered, "the meaning that the term would have to a person of ordinary skill in the art in question at the time of the invention. *See Phillips v. AWH Corp.*, 415 F.3d 1303, 1315 (Fed. Cir. 2005) (en banc) (internal quotations omitted) (citing *Innova/Pure Water, Inc. v. Safari Water Filtration Systems, Inc.*, 381 F.3d 1111 (Fed. Cir. 2004)). Further, "[d]uring examination, claims are to be given their broadest reasonable

interpretation consistent with the specification, and claim language should be read in light of the specification as it would be interpreted by one of ordinary skill in the art." In re *American Academy of Science Tech. Center*, 367 F.3d 1359, 1363 (Fed. Cir. 2004) (citing *In re Bond*, 910 F.2d 831, 833 (Fed. Cir. 1990)). The customary definition of a file system in the art is an I/O interface structure which provides access to directories. This definition of a file system is consistent with the Specification. *See* Specification, paragraph [0058].

1b. A first file system and a second file system refer to two distinct file systems

Specifically, as described above, a file system includes an I/O interface structure and corresponding directories. Thus, the application requires the first and second file system to include a first and second I/O interface, respectively. However, the Examiner cites the host file system and restricted file system of Dalton as disclosing the two file systems of the claimed invention. *See* Final Rejection p. 4. However, the restricted file system of Dalton is merely a subset of the host file system. Specifically, Dalton defines the restricted file system as "a non-overlapping restricted subset of the main file system." Said another way, the restricted file system of Dalton fails to disclose a second I/O interface. This is clearly distinguishable from the claimed invention, which requires two separate file systems and, as such, two separate I/O interfaces.

Further, the Examiner's interpretation of a first and second file system renders the term "second file system" meaningless. Specifically, Dalton never discloses a second file system. Rather, Dalton discloses a single file system which may be restricted. By construing the second file system as a restriction of the first file system, the Examiner is rendering the term, "second

file system" meaningless. Thus, the Examiner has failed to identify a first and second file system in Dalton.

2. Dalton fails to disclose all the limitations of independent claim 1, as arranged in the claim

Appellants respectfully assert that, even assuming, *arguendo*, that the host file system and restricted file system of Dalton disclose the first and second file systems of the claimed invention, the Examiner's rejection still fails because the host file system and restricted file system are not arranged as required by the claim.

2a. Proper Construction of "global zone," and "non-global zone."

Appellants respectfully assert that "[t]he claims, or course, do not stand alone. Rather, they are part of a fully integrated writing instrument … consisting principally of a specification that concludes with the claims. For that reason, claims must be read in view of the specification, of which they are part." *Phillips v. AWH Corp.*, 415 F.3d 1303, 1315 (Fed. Cir. 2005) (en banc) (internal quotations omitted) (citing *Markman v. Westview Instruments*, 52 F.3d 967 (Fed. Cir. 1995)). In view of the Specification, the terms "global zone," "non-global zone," and "file system" have distinct meanings.

Regarding the term "global zone," the term is defined in the originally filed Specification as "the general [operating system] environment that is created when the OS is booted and executed, and serves as the default zone in which processes may be executed if no non-global zones 140 are created." *See* Specification, para. [0033]. Thus, the proper construction of the term "global zone" is the general operating system environment.

Regarding the term "non-global zone," the originally filed Specification specifically states that the non-global zones "represent separate and distinct partitions of the OS

environment." *See* Specification, para. [0034]. Further, non-global zones provide isolation for entities, "such as processes, one or more file systems, and one or more network interfaces." *See* Specification, para. [0034].

2b. The global zone, non-global zone, and file systems are not arranged in the prior art as required by the invention.

Appellants respectfully assert, "[u]nless a reference discloses within the four corners of the document not only all to the limitations claimed but also all of the limitations arranged or combined in the same way as recited in the claim, it cannot be said to prove prior invention of the thing claimed and, thus, cannot anticipate under 35 U.S.C. § 102." *Net MoneyIN v. Verisign*, 545 F.3d 1359, 1371 (Fed. Cir. 2008).

Appellants assert that the host file system of Dalton, and the subset of the host file system, are not arranged or combined in the same way as the first and second file system of the claimed invention. Specifically, the claimed invention requires that a first file system is located within a non-global zone and a second file system is located within a global zone.

Dalton discloses a single file system with various restricted subsets. Because there is only one file system it can only be located in a single execution environment. As such, the file system in Dalton may, at best, be construed as operating in a global zone. From this it follows that the entire file system, including the restricted portion of the file system (which the Examiner contends is equivalent to the second claimed file system) is located in the global zone.

Accordingly, Dalton does not include a second file system located in a distinct execution environment (*i.e.,* the non-global zone) as required by the claims. Because the elements in Dalton are not arranged or combined in the same way as recited in the claim, the rejection fails to

satisfy the requirements set forth in *Net MoneyIN*. Thus, the rejection is improper and should be reversed.

VIII. CONCLUSION

In view of the above, the Examiner's contentions do not support the rejection of claims 41, 47, 48, 50, and 53-58 under 35 U.S.C. §102(e). Accordingly, a favorable decision from the Board is respectfully requested.

Dated: May 10, 2010

Respectfully submitted,

By /Robert P. Lord/
Robert P. Lord
Registration No.: 46,479
OSHA · LIANG LLP
3945 Freedom Circle, Suite 300
Santa Clara, California 95054
(408) 727-0600
(408) 727-8778 (Fax)
Attorney for Applicant

CLAIMS APPENDIX

Claims involved in Appeal.

1. – 40. (Canceled)

41. A computer readable medium comprising a set of one or more instructions which, when executed by one or more processors, cause the one or more processors to perform the method of:

in an operating system environment controlled by a single operating system kernel instance, establishing a global zone comprising a first non-global zone, wherein the first non-global zone comprises a first file system and wherein the global zone comprises a second file system;

receiving, from a first process, a first request to perform a first operation, wherein the first process is associated with a first set of privileges and is executed by at least one of the one or more processors, and wherein the first set of privileges restrict the first process to the first non-global zone;

in response to the first request, determining whether performing the first operation is within the first set of privileges; and

denying the first request if performing the first operation is not within the first set of privileges.

42. – 46. (Cancelled)

47. The computer readable medium of claim 41, wherein performing the first operation comprises accessing an object, the method further comprising:

determining whether the first process has permission to access the object.

48. The computer readable medium of claim 41, wherein the first operation includes one of:

mounting/unmounting a file system, overriding file system permissions, binding to a privileged network port, and controlling other processes with different user identifiers.

49. (Cancelled)

50. The computer readable medium of claim 41, wherein the method further comprises:

receiving, from a second process associated with a second set of privileges, a second request to perform a second operation, wherein the second process is executing in the global zone, and wherein the second process is executed by at least one of the one or more processors;

in response to the second request, determining whether performing the second operation is within the second set of privileges; and

denying the second request if performing the second operation is not within the second set of privileges.

51. (Cancelled)

52. (Cancelled)

53. The computer readable medium of claim 50, wherein the second operation includes one of:

modifying all process privileges, writing to system administration file, opening device holding kernel memory, modifying operating system code, accessing file systems restricted to root user, setting the system clock, changing scheduling priority of an executing process, reserving resources for an application, directly accessing a network layer and loading kernel modules.

54. A system, comprising:

at least one processor; and

a computer readable medium, comprising a set of instructions which, when executed by the at least one processor, cause the at least one processor to perform the method of:

in an operating system environment controlled by a single operating system kernel instance, establishing a global zone comprising a first non-global zone, wherein the first non-global zone comprises a first file system and wherein the global zone comprises a second file system;

receiving, from a first process, a first request to perform a first operation, wherein the first process is associated with a first set of privileges and is executed by at least one of the one or more processors, and wherein the first set of privileges restrict the first process to the first non-global zone;

in response to the first request, determining whether performing the first operation is within the first set of privileges; and

denying the first request if performing the first operation is not within the first set of privileges.

55. The system of claim 54, wherein performing the first operation comprises accessing an object, the method further comprising:

determining whether the first process has permission to access the object.

56. The system of claim 54, wherein the first operation includes one of:

mounting/unmounting a file system, overriding file system permissions, binding to a privileged network port, and controlling other processes with different user

57. The system of claim 54, wherein the method further comprises:

receiving, from a second process associated with a second set of privileges, a second request to perform a second operation, wherein the second process is executing in the global zone, and wherein the second process is executed by at least one of the one or more processors;

in response to the second request, determining whether performing the second operation is within the second set of privileges; and

denying the second request if performing the second operation is not within the second set of privileges.

58. The system of claim 57, wherein the second operation includes one of:

modifying all process privileges, writing to system administration file, opening device holding kernel memory, modifying operating system code, accessing file systems restricted to root user, setting the system clock, changing scheduling priority of an executing process, reserving resources for an application, directly accessing a network layer and loading kernel modules.

EVIDENCE APPENDIX

NONE

RELATED PROCEEDINGS APPENDIX

NONE